JPAS ACCOUNT REQUEST PROCEDURES

Last updated 8/13/2012

Table of Contents

New JPAS Account Checklist

The following is a quick reference checklist to assist prospective JPAS users in completing the required steps for a JPAS account.

- □ Meet clearance requirements
  The minimum requirement for JPAS access is Secret eligibility. JAMS users, Levels 2, 3 and 8 require an SSBI at minimum.

- □ Take JPAS training
  - □ JPAS/JAMS Virtual Training for Security Professionals, STEPP course PS124.06
    http://www.dss.mil/cdse/catalog/elearning/PS124.html

  - □ JPAS/JCAVS Virtual Training for Security Professionals, STEPP course PS123.16
    http://www.dss.mil/cdse/catalog/elearning/PS123.html

- □ Take PII training, STEPP course DS-IF101.06
  http://www.dss.mil/cdse/catalog/elearning/DS-IF101.html

- □ Complete SAR Form

- □ Submit LOA, if applicable
  A Letter of Appointment (LOA) is required for Industry, DoD Agency and Non-DoD Government Agency JPAS account applicants. Military account applicants are not required to submit an LOA at this time.

Once all elements in the list are completed, please refer to the instructions below to submit your documentation to the appropriate JPAS Account Manager. **DO NOT** submit requests to the DoD Security Services Center (JPAS Call Center) unless you meet the requirements in the **Industry Account Managers** section of this document.

How Do I Obtain a JPAS Account?

Military

To obtain a new JPAS account required to perform your job duties on behalf of a military branch (applicants may be active duty military, civilians or contractors), you will need to contact an established JPAS Account Manager within your military branch. If you do not know whom to contact, please refer to the JPAS POC Listing on the DMDC JPAS User web site to locate a JPAS PMO for your military branch. To request an account, your JPAS Account Manager will need:

- A JPAS System Access Request (SAR) form must be completed, signed, and submitted. The signatures need to be your Commanding Officer, your Security Officer, and the applicant. To obtain a copy of the SAR form, navigate to the SAR Form section of this document.

DoD Agencies

To obtain a new JPAS account required to perform your job duties on behalf of a DoD Agency (applicants may be active duty military, civilians or contractors), you will need to contact your agency's JPAS Account Manager and/or Facility Security Officer (FSO) to process your request. To request an account, your JPAS Account Manager will need:

- A Letter of Appointment (LOA) on your agency's letterhead indicating who the account is for and the specific job duties that require JPAS access. Your Agency's Director or delegate must sign the letter. Delegates must be GS-14 grade (or agency equivalent) or higher. One LOA may be created for multiple applicants if they share common job duties that require JPAS access.
- A JPAS System Access Request (SAR) form must be completed, signed, and submitted. The signatures need to be your Agency's Director or delegate, your Security Officer, and the applicant. To obtain a copy of the SAR form, navigate to the SAR Form section of this document.

Industry

Users: To obtain a new JPAS account required to perform your job duties on behalf of an Industry company, you will need to contact your company's JPAS Account Manager or FSO. Your JPAS Account Manager will process your request. To request an account, your JPAS Account Manager will need:

- A Letter of Appointment (LOA) on your company's letterhead indicating who the account is for and the specific job duties that require JPAS access. A Corporate Officer or Key Management Personnel (KMP) listed in Industrial Security Facilities Database (ISFD) must sign the letter. One LOA may be created for multiple applicants within the same company if they share common job duties that require JPAS access.
- A JPAS System Access Request (SAR) form must be completed, signed, and submitted. The signatures need to be your Corporate Officer, your Security Officer, and the applicant. To obtain a copy of the SAR form, navigate to the SAR Form section of this document.

Account Managers: If an Account Manager already exists at your company, they will process your request. Requests for additional Account Managers should **not** be submitted to the DoD Security Services Center (JPAS Call Center). If there are **no** existing Account Managers or FSOs for your company, you will follow the process below and request to be the primary Account Manager for your company. The JPAS Call Center will create your account. To request an account, you will need to submit two (2) items:

- A Letter of Appointment (LOA) on your company's letterhead naming the applicant as the company's primary JPAS Account Manager. A Corporate Officer or Key Management Personnel (KMP) listed in Industrial Security Facilities Database (ISFD) must sign the letter.
- A JPAS System Access Request (SAR) form must be completed, signed, and submitted. The signatures need to be your Corporate Officer, your Security Officer, and the applicant. To obtain a copy of the SAR form, navigate to the SAR Form section of this document.

After completing a SAR and the LOA, please submit both to the JPAS Call Center, as described in the Submitting the SAR Form section of this document. Once the account has been created, the JPAS Call Center will contact you with your initial log-in credentials. Please review the Most Common Reasons for SAR Rejection/Disapproval section prior to submitting your SAR and LOA.

Non-DoD Government Agencies

To obtain a new JPAS account required to perform your job duties on behalf of a Non-DoD Agency (applicants may be civilians or contractors), you will need to submit three (3) items:

- Proof of your security clearance

- A Letter of Appointment (LOA) on your agency's letterhead indicating who the account is for and the specific job duties that require JPAS access. Your Agency's Director or delegate **must** sign the letter. Delegates must be GS-14 grade (or agency equivalent) or higher.
- A JPAS System Access Request (SAR) form must be completed, signed, and submitted. The signatures need to be your Agency's Director or delegate, your Security Officer, and the applicant. To obtain a copy of the SAR form, navigate to the SAR Form section of this document.

The SAR, LOA, and proof of your security clearance (if not in JPAS) must be submitted to the JPAS Call Center, who will forward it to the JPAS Program Manager (PM). The JPAS PM will deny/approve the request and forward to the JPAS Support Team (JST) for processing if approved. The JST will contact you with your initial log-in credentials.

JPAS Account Policies

Account Activity

- **Active JPAS Account**:
  An active JPAS account is one that has been logged into in the past 30 days.

- **Inactive JPAS Account**:
  An inactive JPAS account is an account that has not been logged into in the past 60 days. If a JPAS account is inactive for 60-89 days, the JPAS system will automatically lock the account. Only the company/agency Account Manager overseeing the user's account will be able to unlock the account.

- **Deleting of Inactive JPAS Accounts**:
  JPAS accounts that have not been logged into for longer than 90 days are deleted per DoD Regulations (DISA APP6240). If a JPAS account is needed, a new account will have to be established following the aforementioned request procedures.

Violations/Misuse of JPAS Accounts

By using the JPAS application, users are consenting to the terms of use of the application and are agreeing to maintain compliance with the Privacy Act of 1974 and all applicable JPAS rules and regulations, including the JPAS Account Management Policy.

Misuse of JPAS will result in termination of the offender's JPAS account, exclude culpable companies or persons from future access to JPAS, and offenders will have a technology incident recorded on their JPAS record. Information concerning violations of JPAS policies may also be referred to other federal agencies for consideration of administrative, civil, or criminal sanctions when circumstances warrant.

Common misuses of JPAS include, but are not limited to:

- Sharing of username, password, CAC or PIV cards and/or associated PIN numbers to access the system
- Allowing non-cleared individuals to access the system
- Leaving the JPAS application unsecured while logged into it
- Allowing personnel to view data on the JPAS screen that do not have the proper authorization
- Providing printouts of JPAS data

- Querying the JPAS application for information of which you have *no need to know* to conduct your official duties

System Access Request (SAR) Form

The SAR form and Letter of Appointment (LOA) are required for a JPAS account and must be signed by the appropriate individuals. NOTE: LOA is not required for military user account applicants.

Most Common Reasons for SAR Rejection/Disapproval

The following outlines the most common reasons for JPAS Call Center rejection/disapproval of the JPAS (JCAVS) SAR form. Avoiding these pitfalls will enhance the processing/approval timeline of your SAR submission, if account/access eligibility requirements are met.

1. **No (or Incomplete) Letter of Appointment (LOA) Submitted with SAR (Industry primary Account Managers)** –
   The LOA must be drafted on company letterhead, name the applicant as the company's primary Account Manager, and be signed by a Key Management Personnel (KMP). The same KMP **must** sign both the SAR, as Nominating Official, and the LOA.

2. **Nominating Official is Not Key Management Personnel (KMP) in ISFD** –
   For Industry, the Nominating Official signature in the SAR must belong to a company KMP listed in the Industrial Security Facilities Database (ISFD).

3. **Industry User or Additional Industry Account Manager, DoD Agency, or Military Request** –
   These requests must be submitted within your military branch, company, or agency to the appropriate Account Manager with authority to create a JPAS account. The JPAS Call Center is not authorized to create these accounts in lieu of the responsible Account Manager.

4. **Missing Signatures** –
   All three signatures **must** be present on the SAR form. The three signatures boxes are: User Certification (the applicant), Nominating Official Certification (the KMP, Corporate Officer, or Agency Director), and the Validating Official's Verification (verifying your clearance information is accurate). NOTE: The JPAS Call Center will complete the Validating Official's Verification box on the SARs it processes (primary Account Managers within Industry companies).

5. **Obsolete SAR Form Submitted** –
   Only DSS Form 273, dated June 2011, will be accepted/processed. All other SAR forms will be rejected.

6. **Applicant Already Possesses an Account** –
   Prior to submitting a request for JPAS access, applicant should verify with their JPAS Account Manager to determine if an account already exists. If you do not have a JPAS Account Manager, then you may verify with the JPAS Call Center.

7. **Applicant Not Eligible Due to Security Clearance** –
   At a minimum, an Interim Secret Clearance with an open investigation is required to possess a JPAS account. Applicant should not submit a SAR form until they have been granted at least an Interim Secret Clearance.

8. **Applicant Not Eligible For Requested Level** –
If Applicant has requested a Level 2, 3 or 8 account, which requires TS SCI, and has not been briefed in JPAS at a TS SCI level, the SAR will be rejected. Applicants should verify their clearance level prior to submitting the SAR.

9. **CAGE Code Not Listed in ISFD** –
The CAGE code listed on the SAR could not be found in ISFD. The CAGE code must be listed in ISFD, because the facility must be cleared and the Nominating Official must be verifiable in ISFD as a KMP.

10. **SSN Not Located in JPAS** –
The social security number (SSN) on the SAR was not located in JPAS. This would indicate either the SSN was entered incorrectly on the SAR or the applicant does not meet the minimum JPAS account eligibility/access requirements (does not have a record in JPAS).

Submitting the SAR Form and LOA

The LOA and completed SAR form (to include all three signatures) should be submitted to your company/agency JPAS Account Manager IAW the policy outlined above. NOTE: LOA is not required for military applicants.

Those applicants who meet the requirements to send to the JPAS Call Center can submit the completed SAR and LOA to:

Fax number: (703) 493-8965

Email: account.request@dsshelp.org
If you choose to submit your SAR via unencrypted email, your PII will be at risk.

Mailing address:
DoD Security Services Center
10430 Furnace Road, Suite 101
Lorton, VA, 22079

If the SAR and LOA are not completed per the policy or applicants submit to the JPAS Call Center instead of their existing Account Manager, the JPAS account request will be denied.

Complete the SAR Form

The SAR form (DSS Form 273, dated June 2011) is available at the following link.